TURING 图灵程序设计丛书

Developing Secure
Web Applications

[日] 德丸浩 / 著 赵文 刘斌 / 译 OWASP子明 / 审

Web应用安全权威指南

日本Web应用安全第一人扛鼎力作!!

OWASP北京区负责人、51CTO信息安全专家 作序推荐

在虚拟机上亲自体验攻击流程

人民邮电出版社
POSTS & TELECOM PRESS

TURING 图灵程序设计丛书

[日] 德丸浩 / 著
赵文 刘斌 / 译
OWASP子明 / 审

Web应用安全

权威指南

人民邮电出版社
北京

图书在版编目(CIP)数据

Web应用安全权威指南 /(日)德丸浩著；赵文，刘斌译. -- 北京：人民邮电出版社，2014.10
(图灵程序设计丛书)
ISBN 978-7-115-37047-1

Ⅰ. ①W… Ⅱ. ①德… ②赵… ③刘… Ⅲ. ①网页制作工具 Ⅳ. ①TP393.092

中国版本图书馆CIP数据核字(2014)第206409号

内 容 提 要

本书系日本Web安全第一人德丸浩所创，是作者从业多年的经验总结。作者首先简要介绍了Web应用的安全隐患以及产生原因，然后详细介绍了Web安全的基础，如HTTP、会话管理、同源策略等。此外还重点介绍了Web应用的各种安全隐患，对其产生原理及对策进行了详尽的讲解。最后对如何提高Web网站的安全性和开发安全的Web应用所需要的管理进行了深入的探讨。本书可操作性强，读者可以通过下载已搭建的虚拟机环境亲自体验书中的各种安全隐患。

本书适合Web相关的开发人员特别是安全及测试人员阅读。

◆ 著　[日]德丸浩
译　赵　文　刘　斌
审　OWASP子明
责任编辑　乐　馨
执行编辑　杜晓静
责任印制　焦志炜
◆ 人民邮电出版社出版发行　北京市丰台区成寿寺路11号
邮编　100164　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京鑫正大印刷有限公司印刷
◆ 开本：800×1000　1/16
印张：25
字数：591千字　2014年10月第1版
印数：1-4 000册　2014年10月北京第1次印刷
著作权合同登记号　图字：01-2014-0494号

定价：79.00元

读者服务热线：(010)51095186转600　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京崇工商广字第0021号

推荐序

我投身信息安全产业领域已经有十五个年头了。过去我通过端口扫描，探测服务器的操作系统类型；防火墙出现后，我又转攻 Web 应用安全，结交了很多业内的顶级信息安全专家，与他们进行了大量的交流。

互联网的出现使得大家从传统的纸质信件传递转变为通过互联网电子邮件收发邮件；社交网络的出现，让我们得以通过互联网来结交更多的朋友。然而，我们在享受这些便利的同时，也承受着恶意钓鱼、跨站脚本攻击、恶意网马植入等风险。这些行为造成用户的信息泄漏，银行卡、信用卡信息被恶意盗刷，以致产生大量的经济损失。

通过国际权威的 Web 应用安全机构 OWASP 所发布的 TOP Ten，可以看出 Web 安全的重要性。现在全球有效的网络攻击中，基于 Web 的占 80%，SQL 注入与跨站脚本攻击一直都位于 OWASP Top Ten 的前两名，这两种攻击通常都发生在 Web 应用当中。

本次受图灵公司的邀请，参与了本书的校译工作，在进行校译期间看到了赵文和刘斌两位译者深厚的日文专业技术功底，同时也深深地感受到了日本人工作的严谨，作者在书中为大家准备了详实的应用案例和代码。

我作为 OWASP 中国北京的负责人，有幸组织和参与了在中国区域内召开的信息安全峰会与亚洲应用安全峰会，发现国外的信息安全专家更善于总结。他们能通过有效的方法论有效地进行一些精尖技术的推广和学习，而国内的信息安全专家在介绍一些高精技术时一般只告知结果，而不介绍过程。

《Web 应用安全权威指南》这本书的作者是日本 Web 安全第一人，足见其编程功底之深厚。本书没有欧美作者的那些诙谐幽默的用语，更多的是严谨而实用的陈述。作者以 Web 应用的安全隐患为引子，将产生安全隐患的原因作为整个主线来描述，同时还生动地介绍了试验这些安全隐患的环境的搭建，以及缺陷代码的示例。同时本书又给大家做了很好的补充说明，讲述了 Web 安全的基础协议和原理，帮助读者打好 Web 安全的基本功。

最难能可贵的是，本书详尽地讲解了 SQL 注入、XSS、CSRF 等的基本原理，同时又增加了详尽的代码解析。这是一本难得的 Web 应用安全指南。无论你是 Web 安全的爱好者，还是研究者，都可以将它作为一本很好的参考书籍。个人建议一些高校的学生通过学习本书，实现从 Web 安全的基础入门到精通。

OWASP 中国北京区负责人、51CTO 信息安全专家

陈亮（OWASP 子明）

译者序

2011 年，索尼遭受了 3 次大规模攻击，造成 7700 万 PlayStation Network（PSN）用户的个人信息泄漏。攻击令 PSN 网络服务瘫痪了 23 天，给索尼造成了上亿美元的经济损失。

2011 年 12 月，国内知名开发者社区 CSDN 遭到攻击，600 万用户账号及明文密码泄漏并在网络上被大量传播。

2013 年 3 月，全球知名的云笔记应用 Evernote 遭到攻击，导致 5000 万用户的邮箱地址和加密密码泄漏。

写下这篇文字时，又正值全球最大的众筹网站 Kickstarter 被攻击而导致用户信息被窃取。

一件件触目惊心的事件无一不在提醒着我们网络安全的重要性。造成这些事件的罪魁祸首或许只是代码中一些不起眼的地方，但引发的影响及后果却骇人听闻。掌握如何在编程时不引入漏洞已成为了 Web 应用开发者不可或缺的技能。

然而，当开发者想要系统性地学习 Web 应用安全时，却发现市面上充斥着以攻击者的视角写作的“XX 攻防大全”等书籍，却鲜有站在开发者立场的优秀的权威性书籍可供参考。图灵公司引进的这本《Web 应用安全权威指南》正好填补了这一领域的空缺。

“在那本‘德丸本’中有透彻的讲解。”这是译者在日本工作期间，向同事询问“什么是 CSRF”时得到的答复。没错，“德丸本”就是本书在日本的昵称，几乎在每个 Web 开发小组的案头都能发现它的身影。

本书的作者德丸浩先生在日本被誉为“Web 应用安全领域第一人”，他在经营着一家 Web 安全咨询公司的同时，还在博客上笔耕不辍，孜孜不倦地分享着自己 Web 安全方面的知识，得此称号可谓实至名归。这本书是目前为止德丸浩先生出版的唯一一本图书，可以说是从业多年的经验沉淀下来的精华。

看过日系技术书的读者，一定会对其通俗易懂、深入浅出、谦虚谨慎等特点印象深刻，本书也不例外。SQL 注入、XSS、CSRF 等对于 Web 开发人员来说耳熟能详却可能一知半解的术语，都将在这本书中详细剖析。本书既适合从头到尾通读来进行系统性学习，也适合作为参考书时常查阅。

最后，再一次感谢图灵文化的编辑们能将这本书引入到国内。感谢另一位译者刘斌的辛勤付出，使得本书能够成功地问世。还要感谢妻子马超对我使用业余时间进行翻译工作的鼓励和支持。

希望本书能够让您受益。

赵文

2014 年 2 月于无锡

前言

近年来，利用 Web 应用存在的安全隐患（即所谓的“漏洞”）展开攻击的案例层出不穷，受害者也与日俱增。虽说只要消除安全隐患就能够杜绝这些攻击，但这就需要 Web 应用开发人员掌握正确的安全性方面的知识。

目前，网络上充斥着大量关于安全性的信息，但多数内容都只是流于表面，无法解答开发人员的困惑。具体来说，主要存在以下几点疑问。

- 为什么会产生安全隐患
- 安全隐患会产生什么样的影响
- 如何编程才能消除安全隐患
- 为什么某些方法能够消除安全隐患

而本书就是为了解答这些疑问而创作的。为此，从安全隐患产生的原理到具体的对策，以及采用该对策的根据，本书都将尽可能地详细讲述。本书的目标读者包括程序员、设计师、项目经理、质量管理负责人等参与 Web 应用开发的全部人员。另外，本书也会站在 Web 应用的发包方（甲方）的立场上，尽可能地为其提供有用的信息。

虽然本书面向的是开发人员，但对攻击的手段也做了详细的解说。目的就是为了能够让读者切实感受到安全隐患所造成的影响。但有一点需要注意的是，如果没有得到网站管理员的许可就尝试实施攻击的话，就有可能会触犯相关的法律法规。由于非专业人员很难判断自己的行为是否违法，因此，请不要在没有得到许可的情况下攻击正式的网站。

为了让读者能够放心地体验攻击流程，本书提供了在 VMware Player 的虚拟机环境中尝试安全隐患攻击的方法。希望读者能够通过亲自动手，来加深对安全隐患的理解。

最后，虽然本书中的示例代码主要使用了 PHP 语言，但讲述的内容对其他语言也是同样适用的。

谢辞

笔者在写作本书时，在网上征集了一些试读者，并根据试读者的意见和反馈不断地进行了调整。试读者不仅指出了错别字及语法问题，还提出了各种各样的改进方案，甚至还就安全隐患进行了深入的探讨，实在令笔者受益匪浅。如果没有这些建议和探讨，本书就不会是现在的样子。衷心感谢以下这些试读者（恕笔者省略敬称）：

大崎雅幸、太田良典、kaito834、加藤泰文、小邨孝明、坂井隆二、下冈叶子、高木正弘、竹迫良范、东内裕二、塙与志夫、日野洋一郎、山崎圭吾、山下太郎、Masahiro Yamada（masa141421356）、山本阳平

另外，长谷川阳介先生对本书提出了宝贵意见。同时笔者还在 Twitter 上收到了很多人士的建议。在此一并表示感谢。

最后还要感谢本书的编辑——SB Creative 股份有限公司信息书籍编辑部的友保健太先生，友保先生不仅对写作进度缓慢的笔者颇为照顾，还时常给出宝贵的意见和建议。在此向您致以衷心的感谢。

2011 年 1 月

德丸浩

目录